Projective Ring Line of a Specific Qudit

Hans Havlicek[1] and Metod Saniga[2]

[1]Institut für Diskrete Mathematik und Geometrie
Technische Universität Wien, Wiedner Hauptstrasse 8-10
A-1040 Vienna, Austria
(havlicek@geometrie.tuwien.ac.at)

[2]Astronomical Institute, Slovak Academy of Sciences
SK-05960 Tatranská Lomnica, Slovak Republic
(msaniga@astro.sk)

Abstract

A very particular connection between the commutation relations of the elements of the generalized Pauli group of a d-dimensional qudit, d being a product of distinct primes, and the structure of the projective line over the (modular) ring $\mathbb{Z}_d$ is established, where the integer exponents of the generating shift (X) and clock (Z) operators are associated with submodules of $\mathbb{Z}_d^2$. Under this correspondence, the set of operators commuting with a given one — a perp-set — represents a $\mathbb{Z}_d$-submodule of $\mathbb{Z}_d^2$. A crucial novel feature here is that the operators are also represented by *non*-admissible pairs of $\mathbb{Z}_d^2$. This additional degree of freedom makes it possible to view any perp-set as a *set-theoretic* union of the corresponding points of the associated projective line.

PACS Numbers: 03.65.-a – 03.65.Fd – 02.10.Hh – 02.40.Dr
Keywords: Qudit – Generalized Pauli Group – Projective Ring Line – Commutation Algebra of Generalized Pauli Operators

1 Introduction

The study of the finite-dimensional Hilbert spaces and their associated generalized Pauli operators has been a forefront issue of the quantum information theory within the past few years. A substantial mathematical insight has been possible thanks to a number of novel graph-combinatorial and algebraic geometrical concepts employed, see, e. g., [1]–[6] and references therein. Among the latter, it is the concept of a projective line defined over a(n associative) ring with unity that acquired a distinguished footing [6]–[12]. In this approach, one simply

identifies the points of a projective ring line with the generalized Pauli operators (or the maximum commuting sets of them) pertaining to a given Hilbert space and rephrases their commutation relations in terms of neighbour/distant relations between the points on the line in question. Given this identification, it was possible to "projective-ring-geometrize" any N-qubit Hilbert space [6]–[10], two-qutrits [11, 12], as well as to get important hints about the smallest composite case, viz. a six-dimensional Hilbert space [13]. A detailed examination of these particular cases led soon to a discovery of a more complex and unifying approach based on group-theoretical considerations [14, 15]. Adopting and properly generalizing the strategy pursued in the last two mentioned papers, we shall demonstrate, on the example of a specific single qudit, that the concept of a projective ring line naturally emerges also in a context slightly different from that introduced and elaborated in [6]–[13], with the finest traits of the structure of the projective line coming into play.

2 The Pauli group G of a single qudit

Let $d > 1$ be an integer and $\mathbb{Z}_d := \{0, 1, \ldots, d-1\}$. Addition and multiplication of elements from $\mathbb{Z}_d$ will always be understood modulo d.

We consider the d-dimensional complex Hilbert space $\mathbb{C}^d$ and denote by

$$\{\, |s\rangle : s \in \mathbb{Z}_d\}$$

a computational basis of $\mathbb{C}^d$. Furthermore, let ω be fixed a primitive d-th root of unity (e. g., $\omega = \exp(2\pi i/d)$).

Now X and Z are unitary "shift" and "clock" operators on $\mathbb{C}^d$ defined via $X|s\rangle = |s+1\rangle$ and $Z|s\rangle = \omega^s|s\rangle$, respectively, for all $s \in \mathbb{Z}_d$. With respect to our computational basis the matrices of X and Z are

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & \omega & 0 & \ldots & 0 \\ 0 & 0 & \omega^2 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & \omega^{d-1} \end{pmatrix},$$

respectively.

The subgroup of the unitary group U_d generated by X and Z, known by physicists as the (generalized) *Pauli group*, will be written as G. The operators $X^0 =: I, X^1, \ldots, X^{d-1}$ form a cyclic subgroup of G with order d; the same properties hold for $Z^0, Z^1, \ldots, Z^{d-1}$. Hence

$$X^{d-1} = X^{-1} \quad \text{and} \quad Z^{d-1} = Z^{-1}. \tag{1}$$

For all $s \in \mathbb{Z}_d$ we have $XZ|s\rangle = \omega^s|s+1\rangle$ and $ZX|s\rangle = \omega^{s+1}|s+1\rangle$. This gives the basic relation

$$\omega XZ = ZX. \tag{2}$$

By virtue of (1) and (2), each element of G, usually referred to as a (generalized) *Pauli operator*, can be written in the *normal form*

$$\omega^a X^b Z^c \quad \text{for some integers} \quad a, b, c \in \mathbb{Z}_d. \tag{3}$$

It is easy to see that this representation in normal form is *unique*: From $\omega^a X^b Z^c = \omega^{a'} X^{b'} Z^{c'}$ follows $\omega^{a-a'} X^{b-b'} Z^{c-c'} = I$. As $|0\rangle$ remains fixed under $Z^{c-c'}$ we obtain $\omega^{a-a'} X^{b-b'}|0\rangle = |0\rangle$. This shows $b - b' = 0$ and $a - a' = 0$. Thus $Z^{c-c'} = I$ which implies $c - c' = 0$, as required. The uniqueness of the normal form (3) will be crucial for our further exhibition.

We immediately may read off from (2) the following rule for multiplication in G, when the factors are given in normal form:

$$(\omega^a X^b Z^c)(\omega^{a'} X^{b'} Z^{c'}) = \omega^{b'c+a+a'} X^{b+b'} Z^{c+c'}.$$

Observe that the product is also in normal form. The term $b'c$ in the exponent of ω on the right hand side shows that G is a non-commutative group. The uniqueness of the normal form implies also that G is a group of order $|G| = d^3$.

The *commutator*[1] of two operators W and W' is

$$[W, W'] := WW'W^{-1}W'^{-1}. \tag{4}$$

If $W = \omega^a X^b Z^c$ and $W' = \omega^{a'} X^{b'} Z^{c'}$ are given in normal form then it is immediate from (2) that

$$[\omega^a X^b Z^c, \omega^{a'} X^{b'} Z^{c'}] = \omega^{cb'-c'b} I. \tag{5}$$

Recall that two operators commute if, and only if, their commutator (taken in any order) is equal to I.

We shall be concerned with two important normal subgroups of G:

The *centre* $Z(G)$ of G is the set of all operators in G which commute with every operator in G. An operator $\omega^a X^b Z^c$ given in normal form lies in $Z(G)$ precisely when (5) holds for any choice of a', b', and c'. Setting $b' := 0$, $c' := 1$ we get $b = 0$, whereas $b' := 1$ and $c' := 0$ gives then $c = 0$. These necessary conditions are also sufficient, whence

$$Z(G) = \{\omega^a I : a \in \mathbb{Z}_d\}.$$

Note that $Z(G)$ is yet another cyclic subgroup of G with order d.

The *commutator subgroup* $[G, G]$ is the smallest subgroup of G which contains all commutators $[W, W']$ with $W, W' \in G$. We follow the usual convention to denote the commutator subgroup of G by G'. From $[Z, X] = \omega I$ follows that all powers of ωI are elements of G'. On the other hand (5) shows that there are no other commutators but the powers of ωI. Altogether we obtain

$$G' = Z(G) = \{\omega^a I : a \in \mathbb{Z}_d\}. \tag{6}$$

[1] We shall always be concerned with commutator of operators in the sense of group theory. It must not be confused with the commutator from ring theory which uses addition and multiplication of operators.

It is easy to see from (5) that each element of G' is indeed a commutator, a property which need not be true for the commutator subgroup of an arbitrary group.

3 The ring associated with G

By expressing the elements of our group G in normal form we saw already that several basic algebraic relations can be expressed solely in terms of the exponents of ω, X and Z. These exponents are always elements of the *ring* $(\mathbb{Z}_d, +, \cdot)$ of integers modulo d. To be more precise, this ring is unital ($1b = b$ for all $b \in \mathbb{Z}_d$) and commutative ($bc = cb$ for all $b, c \in \mathbb{Z}_d$). An element $b \in \mathbb{Z}_d$ is a unit (an invertible element) if, and only if b and d are coprime. If d is a prime then every non-zero element of $\mathbb{Z}_d$ is invertible and $\mathbb{Z}_d$ is a field, otherwise there are non-invertible elements — see, e. g., [16, 17] for more details.

We show now that the ring $\mathbb{Z}_d$ "lives", up to isomorphism, also within our group G. Let us consider the bijective mapping

$$\psi : \mathbb{Z}_d \to G' : a \mapsto \omega^a I.$$

This is an isomorphism of the additive group $(\mathbb{Z}_d, +)$ onto the multiplicative group $(G', \cdot)$, since clearly

$$\psi(a + a') = \omega^{a+a'} I = \psi(a) \cdot \psi(a') \quad \text{for all} \quad a, a' \in \mathbb{Z}_d.$$

However, in $\mathbb{Z}_d$ we also have the binary operation of multiplication. We obtain its counterpart in G' via

$$\psi(aa') = \omega^{aa'} I = (\omega^a I)^{a'} = \psi(a)^{a'} \quad \text{for all} \quad a, a' \in \mathbb{Z}_d.$$

Thus we *could* use the bijection ψ to turn G' into an isomorphic copy of the ring $(\mathbb{Z}_d, +, \cdot)$ by defining "new" binary operations on G in accordance with the two formulas from the above. However, we refrain from doing so in order to avoid misunderstandings. (The "new" addition would be the "old" multiplication.) It is nevertheless important to emphasise that such a construction is possible.

4 A symplectic module associated with G and the commutation algebra of Pauli operators

As $(G, \cdot)$ is a non-commutative group, it cannot be isomorphic to the additive group of any module. Recall that the factor group of G by any normal subgroup is commutative if, and only if, this normal subgroup contains the commutator subgroup G'. This means that the "largest" commutative group we can obtain from G by factorisation is the factor group

$$G/G'.$$

Taking into account our normal form (3) and the description of G' in (6), the group G/G' comprises all cosets

$$G'X^bZ^c \quad \text{where} \quad b,c \in \mathbb{Z}_d. \tag{7}$$

Each element of G/G' can be written in a *unique* way in this *normal form*. As a by-product of this uniqueness, we learn from (7) that the factor group G/G' has order d^2. Multiplication in G/G' is governed by the formula

$$(G'X^bZ^c)(G'X^{b'}Z^{c'}) = G'X^{b+b'}Z^{c+c'} \quad \text{for all} \quad b,c,b',c' \in \mathbb{Z}_d. \tag{8}$$

Let us consider the bijective mapping

$$\varphi : \mathbb{Z}_d^2 \to G/G' : (b,c) \mapsto G'X^bZ^c.$$

Note that the elements of $\mathbb{Z}_d^2$ are written as rows. Sometimes they will be called *vectors*. We now consider $(\mathbb{Z}_d^2, +)$ as a commutative group with the addition $(+)$ defined componentwise. Then (8) establishes immediately that φ is an isomorphism of the additive group $(\mathbb{Z}_d^2, +)$ onto the multiplicative group $(G/G', \cdot)$.

But $\mathbb{Z}_d^2$ is also a module over $\mathbb{Z}_d$ in the usual way. Thus we *could* use the bijections $\psi : \mathbb{Z}_d \to G'$ and $\varphi : \mathbb{Z}_d^2 \to G/G'$ to turn G/G' into an isomorphic module over G'. Like before, it is worth noting that this is possible, but the actual construction will not be needed. Let us just present an example: Given $a,b,c \in \mathbb{Z}_d$ we have on the one hand $a(b,c) = (ab,ac)$. On the other hand the "product" of the "scalar" $\omega^a I \in G'$ with the "vector" $G'X^bZ^c$ would equal the "vector" $G'X^{ab}Z^{ac}$.

Recall that our main goal is to describe whether or not two operators of G commute. Since G/G' is a commutative group, any information of this kind is eliminated by our passage from G to the factor group G/G'. This is why in the following construction we use not only the group G/G', but also the group G and the commutator subgroup G':

Let $G'X^bZ^c$ and $G'X^{b'}Z^{c'}$ be elements of G/G' in normal form. We associate with them the commutator

$$[X^bZ^c, X^{b'}Z^{c'}] = \omega^{cb'-c'b}I \in G'.$$

This assignment uses the group G. It is independent of the choice of representatives from the cosets $G'X^bZ^c$ and $G'X^{b'}Z^{c'}$, since a and a' do not appear on the right hand side of (5).

By virtue of the bijections $\varphi^{-1} : G/G' \to \mathbb{Z}_d^2$ and $\psi^{-1} : G' \to \mathbb{Z}_d$ we are now in a position to transfer this construction to our $\mathbb{Z}_d$-module $\mathbb{Z}_d^2$. This gives a mapping[2]

$$[\cdot,\cdot] : \mathbb{Z}_d^2 \to \mathbb{Z}_d : \big((b,c),(b',c')\big) \mapsto cb' - c'b \tag{9}$$

which just describes the commutator of two elements of G (given in normal form) in terms of our $\mathbb{Z}_d$-module. There are several ways to rewrite the mapping (9),

[2]Of course the symbol $[\cdot,\cdot]$ has two different meanings in (4) and (9).

for example

$$\big[(b,c),(b',c')\big] = (b,c)\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}b'\\ c'\end{pmatrix} = \det\begin{pmatrix}b' & c'\\ b & c\end{pmatrix}. \tag{10}$$

By this formula, the mapping $[\cdot,\cdot]$ is a *bilinear form* on $\mathbb{Z}_d^2$. Clearly, this form is alternating, i. e., $\big[(b,c),(b,c)\big] = 0$ for all $(b,c) \in \mathbb{Z}_d^2$. As usual, we write $(b,c) \perp (b',c')$ if $\big[(b,c),(b',c')\big] = 0$ and speak of *orthogonal* (or: *perpendicular*) vectors (with respect to $[\cdot,\cdot]$). As an alternating bilinear form is always skew symmetric, our orthogonality of vectors is a symmetric relation. As our form $[\cdot,\cdot]$ is *non-degenerate*, i. e., only the zero-vector is orthogonal to all other vectors of $\mathbb{Z}_d^2$, we have indeed a *symplectic module*.

Summing up, we see that the set of operators in G which commute with a fixed operator $\omega^a X^b Z^c$ corresponds to the *perpendicular set* (shortly the *perp-set*) of (b,c), viz.

$$(b,c)^\perp := \big\{(u,v) \in \mathbb{Z}_d^2 : (b,c) \perp (u,v)\big\}.$$

The perp-set of (b,c) is closed under addition and multiplication by ring elements. Also, it is non empty, since

$$\mathbb{Z}_d(b,c) \subset (b,c)^\perp. \tag{11}$$

So, $(b,c)^\perp$ is a $\mathbb{Z}_d$-submodule of $\mathbb{Z}_d^2$. We shall exhibit perp-sets in detail in the following sections.

5 The projective line over $\mathbb{Z}_d$ and the commutation algebra of Pauli operators

In order to say more about perp-sets in $\mathbb{Z}_d^2$ we shall use some basic facts about the projective line over the ring $\mathbb{Z}_d$. We do not need the theory of projective ring lines in its most general form here, since our ring $\mathbb{Z}_d$ is commutative and finite. This will allow to work with determinants and state some definitions in a simpler way. While we sketch here some basic notions and results, the reader is referred to [18]–[22] for further details and proofs.

First, let us consider any vector $(b,c) \in \mathbb{Z}_d^2$. It generates the cyclic submodule

$$\mathbb{Z}_d(b,c) = \{(ub,uc) : u \in \mathbb{Z}_d\}$$

Such a cyclic submodule is called *free*, if the mapping $u \mapsto (ub,uc)$ is injective. In this case the vector (or: pair) (b,c) is called *admissible*. Any free cyclic submodule of $\mathbb{Z}_d^2$ has precisely d vectors, including the zero-vector. However, not all vectors $\neq (0,0)$ of a free cyclic submodule need to be admissible. If (b,c) is an admissible vector then (ub,uc) is also admissible if, and only if, $u \in \mathbb{Z}_d$ is an invertible element. Thus, if d is not a prime each free cyclic submodule of $\mathbb{Z}_d^2$ contains at least one non-admissible vector other than $(0,0)$.

For our ring $\mathbb{Z}_d$ there are several other ways of describing admissible vectors, as the following assertions are equivalent for any vector $(b,c) \in \mathbb{Z}_d^2$:

(a) The vector (b, c) is *unimodular*, i. e., there exist elements $u, v \in \mathbb{Z}_d$ with

$$ub + vc = 1.$$

(b) The vector (b, c) is the first row of an invertible 2×2 matrix with entries in $\mathbb{Z}_d$.

(c) The vector (b, c) is the first vector[3] of a basis of $\mathbb{Z}_d^2$. (This means that there is such a vector $(b', c') \in \mathbb{Z}_d^2$ that the mapping

$$\mathbb{Z}_d^2 \to \mathbb{Z}_d^2 : (u, u') \mapsto u(b, c) + u'(b', c')$$

is a bijection.)

In a more geometric language, motivated by classical analytic projective geometry over the real or complex numbers, a free cyclic submodule of $\mathbb{Z}_d^2$ is called a *point*. The point set

$$\mathbb{P}_1(\mathbb{Z}_d) := \{\mathbb{Z}_d(c, d) : (c, d) \text{ is admissible}\}$$

is the *projective line* over the ring $\mathbb{Z}_d$. According to this definition a point is a set of vectors. In "genuine" projective geometry over a ring the individual vectors contained in a point are of no particular interest. They are merely a useful tool for doing geometry in terms of coordinates. For us, however, the vectors within a point will be significant. This is of course in sharp contrast to Euclid's point of view: *A point is that which has no part.*

Two points $\mathbb{Z}_d(b, c)$ and $\mathbb{Z}_d(b', c')$ of $\mathbb{P}_1(\mathbb{Z}_d)$ are called *distant* if $(b, c), (b', c')$ is a basis of $\mathbb{Z}_d^2$. Two distant points share only the zero vector $(0, 0)$. Otherwise, the points are called *neighbouring*. Thus, two neighbouring points have always a non-zero vector in common.

We are now in a position to state a first, preliminary result about perp-sets.

Theorem 1. *Let $(b, c) \in \mathbb{Z}_d^2$ be any vector and let $\mathbb{Z}_d(b', c')$ be any point of the projective line $\mathbb{P}_1(\mathbb{Z}_d)$ which contains the vector (b, c). Then the following assertions hold:*

(a) *The point $\mathbb{Z}_d(b', c')$ is a subset of the perp-set $(b, c)^\perp$.*

(b) *Under the additional assumption that $\mathbb{Z}_d(b, c)$ is also a point, we have*

$$(b, c)^\perp = \mathbb{Z}_d(b, c) = \mathbb{Z}_d(b', c').$$

Proof. Ad (a): By (11) and the assumption of the theorem, $(b, c) \in \mathbb{Z}_d(b', c') \subset (b', c')^\perp$. We infer from the symmetry of the relation $\perp$ that $(b', c') \in (b, c)^\perp$. Also, since $(b, c)^\perp$ is a submodule, we obtain that the entire point $\mathbb{Z}_d(b', c')$ is a subset of $(b, c)^\perp$.

[3] All bases of $\mathbb{Z}_d^2$ consist of two admissible vectors. In general, a module over a ring may have bases of different size.

Ad (b): As (b,c) is a unimodular vector, there exists a pair $(\widetilde{c},-\widetilde{b}) \in \mathbb{Z}_d^2$ such that $b\widetilde{c}-c\widetilde{b}=1$. This means

$$\det\begin{pmatrix} b & c \\ \widetilde{b} & \widetilde{c}\end{pmatrix} = 1$$

which in turn tells us that (b,c) and $(\tilde{b},\tilde{c})$ form a basis of $\mathbb{Z}_d^2$. Each vector $(u,v) \in \mathbb{Z}_d^2$ can be expressed in a unique way as a linear combination

$$(u,v) = w(b,c) + \widetilde{w}(\widetilde{b},\widetilde{c}) \quad \text{with} \quad w,\widetilde{w} \in \mathbb{Z}_d.$$

By (10), a necessary and sufficient condition for (u,v) to lie in $(b,c)^\perp$ reads

$$\det\begin{pmatrix} wb+\widetilde{w}\widetilde{b} & wc+\widetilde{w}\widetilde{c} \\ b & c\end{pmatrix} = \widetilde{w}(\widetilde{b}c-b\widetilde{c}) = -\widetilde{w} = 0.$$

Therefore $(b,c)^\perp = \mathbb{Z}_d(b,c)$. Finally, we infer from $(b,c) \in \mathbb{Z}_d(b',c')$ that the point $\mathbb{Z}_d(b,c)$ is a subset of the point $\mathbb{Z}_d(b',c')$. These points coincide, as both have precisely d vectors. □

Let us give an example, where $d=6$. We consider the vector $(2,0)$ which cannot be unimodular, because $2b'+0c'=1$ has no solution in $\mathbb{Z}_6$. There are only three distinct multiples of $(2,0)$, namely $(0,0)$, $(2,0)$, and $(4,0)$. This indicates once more that $(2,0)$ is not unimodular (or: admissible). We infer from

$$(2,0) = 4(5,0) = 4(2,3) = 4(5,3)$$

that there are (at least) three points containing $(2,0)$. The subsequent remarks are immediate from Theorem 2 which will be established below. However, their verification is also an easy exercise which can be carried out without any background knowledge: The projective line $\mathbb{P}_1(\mathbb{Z}_6)$ has precisely twelve points. There are no other points containing $(2,0)$ than those mentioned before. The perp-set of $(2,0)$ coincides with the set-theoretic union of those three points, hence

$$\begin{aligned}(2,0)^\perp &= \mathbb{Z}_6(5,0) \cup \mathbb{Z}_6(2,3) \cup \mathbb{Z}_6(5,3) \\ &= \{(5,0),(4,0),(3,0),(2,0),(1,0),(0,0), \\ &\quad (2,3),(4,0),(0,3),(2,0),(4,3),(0,0), \\ &\quad (5,3),(4,0),(3,3),(2,0),(1,3),(0,0)\}.\end{aligned}$$

This is a set of $18-6=12$ vectors, because $(2,0)$, $(4,0)$ and $(0,0)$ are vectors which belong to all three points.

6 A particular case: d is square-free

While Theorem 1 describes the perp-set of any admissible vector, the result for non-admissible vectors is unsatisfactory. The aim of this section is to improve

the results of Theorem 1 under the additional hypothesis that the number d is square-free. Throughout this section we adopt the assumption that

$$d = p_1 p_2 \cdots p_r, \tag{12}$$

where $p_1, p_2, \ldots, p_r$ are $r \geq 1$ distinct prime numbers. The ring $\mathbb{Z}_d$ is isomorphic to the outer direct product

$$\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_r} \tag{13}$$

of r finite *fields*. Let us recall how this isomorphism arises: We consider the ring elements

$$q_k := p_1 \cdots p_{k-1} p_{k+1} \cdots p_r, \quad \text{where} \quad k \in \{1, 2, \ldots, r\}.$$

(For $r = 1$ this product is empty, whence $q_1 = 1$.) The ring $\mathbb{Z}_d$ is the inner direct product of the principal ideals

$$J^{(k)} := \mathbb{Z}_d q_k \quad \text{where} \quad k \in \{1, 2, \ldots, r\}.$$

Given any element $y \in \mathbb{Z}_d$ there exists a unique decomposition

$$y = y^{(1)} + y^{(2)} + \cdots + y^{(r)} \quad \text{with} \quad y^{(k)} \in J^{(k)}.$$

We refer to the elements $y^{(k)}$ as the *components* of y. In terms of this decomposition we can add and multiply elements of $x, y \in \mathbb{Z}_d$ componentwise, i. e.

$$(x + y)^{(k)} = x^{(k)} + y^{(k)} \quad \text{and} \quad (x \cdot y)^{(k)} = x^{(k)} \cdot y^{(k)}.$$

In particular, the unit element $1 \in \mathbb{Z}_d$ has the decomposition

$$1 = 1^{(1)} + 1^{(2)} + \cdots + 1^{(r)}.$$

For each $k \in \{1, 2, \ldots, r\}$ the ideal $J^{(k)}$ is a *field* isomorphic to $\mathbb{Z}_{p_k}$. There is only one isomorphism $J^{(k)} \to \mathbb{Z}_{p_k}$; it takes the element $1^{(k)}$ to the unit element $1 \in \mathbb{Z}_{p_k}$. Note that each element of $J^{(k)}$ can be written as $1^{(k)} + 1^{(k)} + \cdots + 1^{(k)}$ with a finite number of summands. Then its isomorphic image in $\mathbb{Z}_{p_k}$ is the sum $1 + 1 + \cdots + 1$ with the same number of summands. Below we shall always use the representation of $\mathbb{Z}_d$ as the inner direct product of the ideals $J^{(k)}$ rather than the isomorphic model given in (13).

As a first application we obtain the following characterisation: An element $y \in \mathbb{Z}_d$ is invertible if, and only if, all its components are non-zero. In this case the k-th component of the element y^{-1} is the unique solution in $J^{(k)}$ of the equation $y^{(k)} x = 1^{(k)}$ in the unknown x. Therefore the number of invertible elements in $\mathbb{Z}_d$ is

$$\prod_{k=1}^{r} (p_k - 1). \tag{14}$$

A similar description holds for the points of $\mathbb{P}_1(\mathbb{Z}_d)$: A pair (b, c) is unimodular (or: admissible) if, and only if, there exist elements $u, v \in \mathbb{Z}_d$ with

$$u^{(k)}b^{(k)} + v^{(k)}c^{(k)} = 1^{(k)} \quad \text{for all} \quad k \in \{1, 2, \ldots, r\}.$$

Since each ideal $J^{(k)}$ is isomorphic to a field, the last equation is equivalent to

$$(b^{(k)}, c^{(k)}) \neq (0, 0) \quad \text{for all} \quad k \in \{1, 2, \ldots, r\}. \tag{15}$$

We are now in a position to state our main result. Note that the set-theoretic union of points gives a set of vectors.

Theorem 2. *Let the square-free integer $d > 1$ be given as in (12). Also, let $(b, c) \in \mathbb{Z}_d^2$. We denote by K the set of those indices $k \in \{1, 2, \ldots, r\}$ such that $(b^{(k)}, c^{(k)}) = (0, 0)$. Then the following hold:*

(a) *The vector (b, c) is contained in precisely*

$$\prod_{k \in K} (p_k + 1) \tag{16}$$

points of $\mathbb{P}_1(\mathbb{Z}_d)$.

(b) *The set-theoretic union of these points equals the perpendicular set of the vector (b, c).*

(c) *The perpendicular set of the vector (b, c) satisfies*

$$|(b, c)^{\perp}| = d \prod_{k \in K} p_k. \tag{17}$$

Proof. Ad (a): First, let us determine all admissible vectors $(b', c') \in \mathbb{Z}_d^2$ such that $(b, c) = u(b', c')$ for some $u \in \mathbb{Z}_d$. So

$$(b^{(j)}, c^{(j)}) = u^{(j)}(b'^{(j)}, c'^{(j)}) \neq (0, 0) \quad \text{for all} \quad j \in \{1, 2, \ldots, r\} \setminus K \tag{18}$$

and

$$(b^{(k)}, c^{(k)}) = u^{(k)}(b'^{(k)}, c'^{(k)}) = (0, 0) \neq (b'^{(k)}, c'^{(k)}) \quad \text{for all} \quad k \in K. \tag{19}$$

We obtain $u^{(j)} \neq 0$ from (18), whence $(b'^{(j)}, c'^{(j)})$ is one of the $p_j - 1$ distinct multiples of $(b^{(j)}, c^{(j)})$ by a non-zero factor in $J^{(j)}$. Next, (19) implies $u^{(k)} = 0$, whence $(b'^{(k)}, c'^{(k)})$ is one of the $p_k^2 - 1$ non-zero pairs with entries from $J^{(k)}$. These necessary conditions are also sufficient so that we obtain

$$\prod_{j \notin K} (p_j - 1) \prod_{k \in K} (p_k + 1)(p_k - 1)$$

admissible vectors with the required property. Dividing by the number of invertible elements of $\mathbb{Z}_d$, as stated in (14), gives the number of points containing the vector (b, c).

Ad (b): By Theorem 1 (a), each point containing (b, c) is a subset of $(b, c)^\perp$. So the same property holds for the union of all these points. The proof will be accomplished by showing that for any vector $(x, y) \in (b, c)^\perp$ there is a point $\mathbb{Z}_d(b', c') \in \mathbb{P}_1(\mathbb{Z}_d)$ which has (x, y) and (b, c) among its vectors. We define b' and c' in terms of their components as follows: For all $j \in \{1, 2, \ldots, r\} \setminus K$ we let $(b'^{(j)}, c'^{(j)}) := (b^{(j)}, c^{(j)})$. For the remaining indices $k \in K$ we define

$$(b'^{(k)}, c'^{(k)}) := \begin{cases} (x^{(k)}, y^{(k)}) & \text{if } (x^{(k)}, y^{(k)}) \neq (0, 0), \\ (1^{(k)}, 1^{(k)}) & \text{otherwise.} \end{cases}$$

According to our definition and (15) the submodule $\mathbb{Z}_d(b', c')$ is a point. Letting $u^{(j)} := 1^{(j)}$ for all $j \notin K$ and $u^{(k)} := 0$ for all $k \in K$ yields $(b, c) = u(b', c')$.

Finally, we establish the existence of an element $v \in \mathbb{Z}_d$ with $(x, y) = v(b', c')$. For this purpose the components of v can be chosen as follows: If $j \notin K$ then $(x, y) \perp (b, c)$ together with (10) gives

$$\det \begin{pmatrix} x^{(j)} & y^{(j)} \\ b^{(j)} & c^{(j)} \end{pmatrix} = 0.$$

As this is a determinant over the field $J^{(j)}$, and because the second row is non-zero, we can define $v^{(j)} \in J^{(j)}$ via $(x^{(j)}, y^{(j)}) = v^{(j)}(b^{(j)}, c^{(j)})$. If $k \in K$ and $(x^{(k)}, y^{(k)}) \neq (0, 0)$ we set $v^{(k)} := 1^{(k)}$, otherwise we let $v^{(k)} := 0$.

Ad (c): By (b), it suffices to count the number of vectors (b'', c'') which are a multiple of an admissible vector as described in part (a) of the present proof. For each $j \notin K$ the pair $(b''^{(j)}, c''^{(j)})$ can be chosen as any of the p_j multiples of $(b^{(j)}, c^{(j)})$ by a factor in $J^{(j)}$, whereas for each $k \in K$ the pair $(b''^{(k)}, c''^{(k)})$ can be chosen arbitrarily in p_k^2 ways. Hence there are

$$\prod_{j \notin K} p_j \cdot \prod_{k \in K} p_k^2 = d \prod_{k \in K} p_k$$

such vectors. □

As a by-product of Theorem 2 we may infer from (16) that the projective line $\mathbb{P}_1(\mathbb{Z}_d)$ has precisely $\prod_{k=1}^{r}(p_k + 1)$ points. Also, returning to our initial problem, we obtain the following result.

Corollary 1. *With the settings and notations of Theorem 2 the number of operators in the generalized Pauli group G which commute with the operator $\omega^a X^b Z^c \in G$ equals the value given by* (17) *multiplied by d.*

7 Conclusion

Given the generalized Pauli group associated with a d-dimensional qudit, d a product of distinct primes, a general formula was derived for the number of generalized Pauli operators commuting with a given one. This formula is based on the properties of (sub)modules of the associated modular ring $\mathbb{Z}_d$ and finds

its natural interpretation in the properties of the projective line defined over $\mathbb{Z}_d$. When compared with other works on the subject [6]–[13], our approach makes also use of *non*-admissible pairs of elements of the ring in question, thereby giving the physical meaning to the full structure of the line; moreover, it seems to be readily generalizable to tackle the case where d also contains powers of primes.

Acknowledgements

This work was supported by the Science and Technology Assistance Agency under the contract # APVT–51–012704, the VEGA grant agency projects # 2/6070/26 and # 7012 and by the ⟨Action Austria–Slovakia⟩ project # 58s2 "Finite Geometries Behind Hilbert Spaces."

References

[1] PK Aravind, Quantum kaleidoscopes and Bell's theorem, Int J Mod Phys B 2006;20:1711–1729.

[2] A Vourdas, Quantum systems with finite Hilbert space: Galois fields in quantum mechanics, J Phys A: Math Theor 2007;40:R285–R331.

[3] AB Klimov, JL Romero, G Björk and LL Sánchez-Soto, Geometrical approach to mutually unbiased bases, J Phys A: Math Theor 2007;40:3987–3998.

[4] I Bengtsson and K Zyczkowski, Geometry of quantum states: An introduction to quantum entanglement, Cambridge University Press, Cambridge, 2006.

[5] A Klappenecker and M Roetteler, Mutually unbiased bases are complex projective 2-designs, Proc 2005 IEEE International Symposium on Information Theory 2005;1740–1744.

[6] M Planat, M Saniga and M Kibler, Quantum entanglement and projective ring geometry, SIGMA 2006;2:Paper 066.

[7] M Saniga and M Planat, Projective line over the finite quotient ring GF(2)$[x]/\langle x^3 - x\rangle$ and quantum entanglement: Theoretical background, Theor Math Phys 2007;151:474–481.

[8] M Saniga, M Planat and M Minarovjech, Projective line over the finite quotient ring $GF(2)[x]/\langle x^3 - x\rangle$ and quantum entanglement: The Mermin "magic" square/pentagram, Theor Math Phys 2007;151:625–631.

[9] M Saniga, M Planat and P Pracna, Projective ring line encompassing two-qubits, Theor Math Phys 2007; in press, quant-ph/0611063.

[10] M Saniga and M Planat, Multiple qubits as symplectic polar spaces of order two, Adv Studies Theor Phys 2007;1:1–4.

[11] M Planat and M Saniga, Pauli graph and finite projective lines/geometries, Proc. SPIE 2007;6583:65830W.

[12] M Planat and M Saniga, On the Pauli graphs of N-qudits, Quantum Information and Computation 2008;8:127–146.

[13] M Planat, A-C Baboin and M Saniga, Multi-line geometry of qubit/qutrit and higher order Pauli operators, Int J Theor Phys 2007; accepted, 0705.2538 [quant-ph].

[14] K Thas, Pauli operators of N-qubit Hilbert spaces and the Saniga-Planat conjecture, Chaos, Solitons and Fractals 2007, to appear.

[15] K Thas, The geometry of generalized Pauli operators of N-qudit Hilbert space, Quantum Information and Computation 2007, submitted.

[16] BR McDonald, Finite rings with identity, Marcel Dekker, New York, 1974.

[17] R Raghavendran, Finite associative rings, Comp Mathematica 1969;21:195–229.

[18] A Blunck and H Havlicek, Projective representations I: Projective lines over rings, Abh Math Sem Univ Hamburg 2000;70:287–299.

[19] H Havlicek, Divisible designs, Laguerre geometry, and beyond, Quaderni del Seminario Matematico di Brescia 2006;11:1–63, available from ⟨http://www.geometrie.tuwien.ac.at/havlicek/pdf/dd-laguerre.pdf⟩.

[20] M Saniga, M Planat, MR Kibler and P Pracna, A classification of the projective lines over small rings, Chaos, Solitons and Fractals 2007;33:1095–1102.

[21] A Herzer, Chain geometries, in Handbook of incidence geometry, F Buekenhout (ed), Amsterdam, Elsevier, 1995:781–842.

[22] A Blunck and A Herzer, Kettengeometrien — Eine Einführung, Shaker-Verlag, Aachen, 2005.